A Comparative Study of Authentication Methods in Mobile Cloud Computing

G. Reshmi, C.S. Rakshmy
Independent Researchers
India

Abstract

Mobile Cloud Computing (MCC) is an emerging technology which attempts to combine the storage and processing resources of cloud environment with the dynamicity and accessibility of mobile devices. Security, particularly authentication, is fast evolving as a focal area in mobile cloud computing research. This paper comprehensively surveys the various authentication mechanisms proposed so far for mobile cloud computing. We propose a novel classification system for existing authentication methods in MCC. Further, the pros and cons of the various methods are discussed. We present a comparative analysis and recommends future research in improving the surveyed implicit authentication by establishing cryptographic security of stored usage context and actions.

1. Introduction

Cloud computing has emerged as a popular solution to the quest for scalable storage and computing resources in the last decade. Ever since its conception, it has been revolutionizing the way data storage and processing mechanisms are envisioned and implemented. It enabled the on-demand availability of services such as Software, Platform, Infrastructure (through SaaS, PaaS, IaaS respectively) and thus formed an economic solution to meet the ever-fluctuating demand for storage and computational resources by growing businesses.

There are three main deployment models of cloud computing : Private, where the cloud infrastructure is dedicated to a single organization; Public, where the infrastructure is offered via the internet to the general public as free or on a pay-per-usage policy, and Hybrid, where the workloads move between public and private clouds according to changing resource needs. Private clouds deliver a great degree of control and security albeit being a capital-intensive, costly solution. Public clouds, on the other hand, provide maximum efficiency in resource sharing, but raises serious security and privacy concerns. Being a combination of these two deployment models, hybrid clouds offer greater flexibility and data deployment options.

Cloud computing as a business paradigm has gone a long way from the early innovations of Salesforce.com and Amazon web services [1]. Today, a whopping 85% of all software is built for the cloud; 72 % of the developers are reported to use cloud-based APIs and a quarter of all applications are expected to be in the cloud by 2016 [2]. Also, in 2015, $32 billion is calculated to be spent on cloud IT infrastructure per year, according to International Data Corporation, the market intelligence firm [3]. This accounts for 33 percentage of the total IT infrastructure spending. Further, cloud infrastructure spending is expected to reach $52 billion in 2019 which is 45 percentage of the total IT expenditure.

With mobile cloud computing (MCC), we go forward one more step along this way; the dynamic and portable nature of mobile devices is combined with the scalable resource pooling of cloud computing paradigm. It is an amalgamation of mobile computing, cloud computing and wireless networks. The computation and communication intensive operations are offloaded to the cloud, freeing the mobile device from its inherent limitations. MCC is a computing paradigm which helps the mobile device to access and process petabytes of data and run computation-intensive applications which otherwise would have been impossible due to the limitations of the device. Fig. 1 shows the basic structure of mobile cloud computing where mobile devices access cloud services via the internet.

As an emerging technology, it holds great potential albeit with its fair share of issues. Reference [4] examines the challenges in mobile cloud computing in great detail and presents a taxonomy for the same, as follows.

1. Issues on the operational level: methods for offloading, connection protocols, mobility management etc.
2. End user level issues: presentation in the user interface and incentives for collaboration.
3. Service and application level: fault tolerance, performance measurement tools, QoS.
4. Context-awareness: invocation of different cloud services based services.
5. Data management: Personal data could be stored on cloud which must ensure secure multi-tenancy; portability and interoperability of data.

6. Security, privacy and trust: protection against possible misuse of data.

Among these issues, security and privacy is of specific interest to us in this discussion. As in traditional paradigms, authentication plays a major role in security in mobile cloud computing scenarios too. This paper summarizes the existing authentication methods in MCC, presents a classification system for the various methods and points out the advantages and disadvantages of each.

The rest of the paper is organized as follows: Section 2 describes the security concerns in MCC, followed by a brief study of traditional authentication mechanisms in section 3. A comprehensive literature Survey and comparative analysis of the existing *authentication* mechanisms in mobile cloud computing are given in sections 4 and 5 respectively. Section 6 concludes the paper with a summary of the survey done and suggestions for future research.

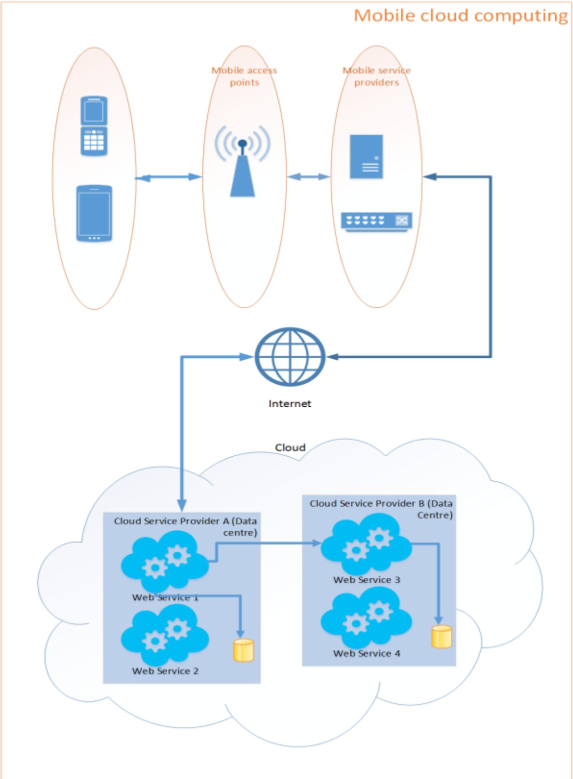

Figure 1. Basic architecture of mobile cloud computing

2. Security in mobile cloud computing

As discussed in [5], MCC inherits the security issues of the cloud computing paradigm whilst being limited by its inherent constraints on resources such as battery life, bandwidth, storage capacity and processing power.

Reference [5] broadly classifies the security issues in MCC into two categories: those for 1) mobile users and 2) data. Security threats to mobile applications through malicious code and privacy issues related to the location based services fall into the first category. This paper further examines the security issues for data stored in the clouds such as integrity, privacy and authentication.

2.1. Security for mobile devices

Mobile devices are susceptible to multiple attacks such as virus, Trojan horse etc. Running an antivirus software to continuously monitor file activities and quarantine suspected malicious code may not be a feasible solution in mobile devices due to the resource limitations.

2.2. Security for data

We can briefly summarize the various security issues in the mobile cloud computing paradigm as follows:

2.2.1. Privacy and confidentiality. Given the amount of personal data stored in mobile phones, data privacy becomes a key issue in mobile cloud scenarios. Privacy of cloud-stored data can be possibly breached by multiple entities including cloud vendors, other users and malicious attackers. In many cases Service Level Agreements are required to provide clauses which prevent cloud vendors from surreptitiously accessing private user data and selling it to third parties without authorization.

2.2.2. Data Migration. Data, often sensitive in nature, is offloaded to the cloud. The exact physical location of data may not be transparent which could lead to complications in jurisdiction scope and privacy commitments. The loss of physical control over the storage of data, combined with multi-tenancy of shared storage devices, potentially with domain competitors can be unnerving for the customers.

2.2.3. Integrity. Data integrity makes sure that the data remains consistent and accurate; it is guarded from illegitimate updates. This is of prime importance in a mobile cloud computing environment where the data could be distributed across multiple data centers, possibly in different geographic locations.

2.2.4. Data Ownership. Specifically in the case of purchased digital media, data ownership is an often-debated issue in mobile cloud computing. Today, users can purchase access to media content using a service; even after purchase, the content may be stored remotely rather than locally. This could give rise to contentions on copyright and ownership issues later, if not carefully handled.

2.2.5. Security and access. Data access and availability becomes key issues in mobile cloud environments as vast majority of data is stored in remote locations. With ever-increasing mobile user requests to access cloud resources, efficient network connectivity and seamless data availability are critical.

2.2.5. Authentication. A related problem is establishing the right data security mechanisms to ensure that only entities with the verified credentials are allowed to access and modify the data. It is the process of confirming the identity of the user who attempts to access a resource or service. It is of prime importance in the mobile cloud computing scenario and in the following sections, we attempt to examine a few traditional and novel mechanisms for authentication in MCC.

3. Traditional authentication mechanisms in the context of mobile cloud computing

Authentication is one of the key aspects of any security system. An authentication service is the ever-vigilant guard at the gateway to the digital fortress; its responsibility is to check the identity of any party seeking entrance (i.e., access) to the system; it verifies certain credentials to ensure that an entity is indeed what it claims itself to be.

In Table 1, we present a comparison of traditional authentication mechanisms with advantages and disadvantages. The magnitude of information stored and processed in a mobile cloud environment provides alluring incentives for an attacker. This, combined with the computational limitations of mobile devices call for traditional authentication methods to be adapted in order to be effective in a mobile cloud environment. We will see details of such adaptations in some of the surveyed papers.

Table 1. Traditional Authentication Mechanisms

Mechanism	**Idea**	**Advantages**	**Disadvantages**
User ID / Password	Pre-registered username and secret password	Simple; popular; easy-to-deploy	Must be renewed frequently
Public Key Infrastructure	Trusted Certificate authority issues private keys	No sharing of secret key	Single point of trust; challenges in scalability
Kerberos	Trusted authority issues tickets	Mutual authentication between client and server	Single point of failure; requires time synchronization
Single Sign-On	One step authentication to multiple applications	User friendly	Any breach in sign-in security affects multiple applications
One Time Password	PIN typically used in multi-factor authentication	Easy-to-use; Compatible with password based authentication	Secure generation and transmission of OTP is challenging
Mobile Trusted Module	Chip for hardware authentication	Optimized for mobile devices; small footprint	Deployment and management is challenging

4. Literature Survey

This survey encompasses most of the major authentication schemes proposed in mobile cloud computing so far. We briefly discuss the principles behind each authentication method. Further, based on the authentication criteria, we propose a classification scheme for the surveyed methods. A comparative analysis of the methods, highlighting the advantages, disadvantages, implementation stage and future research possibilities is given next.

In some of the surveyed frameworks, two or more methods are used sequentially to strengthen the authentication. Alizadeh et al., examine the feasibility of a multi-factor authentication in mobile cloud environment in [6]. The authors enlist limitations of mobile devices and discuss the feasibility of multi-factor authentication with respect it. In particular, the effect of a multi-factor authentication on the performance, power consumption, security and privacy are examined.

The surveyed authentication methods for mobile cloud computing scenario can be broadly classified as follows:

1. User profile methods
2. Cryptographic methods
3. Image-based methods
4. Port-knocking methods

4.1. User profile methods

These methods make use of information about the user for identification. Here, ‘user’ is a generic term; it can mean either the person using the mobile device or the device itself. Typically, user behavioral patterns, biometrics, location information etc. are gathered during a registration phase and verified later for authenticated logins.

Implicit authentication is a relatively new concept which adds the aspect of user’s behavior and activities to the existing standard authentication parameters. Reference [7] extends this concept originally introduced in papers [8] and [9] and merges it with an authentication framework called TrustCube introduced in paper [10]. After briefly summarizing the ideas of implicit authentication and TrustCube, the authors further elaborate on how this can be adopted in a mobile cloud environment, with a high-level architecture and implementation details.

There are four major participants in the proposed system: The Client Device, Authentication Consumer, Authentication Engine and Data Aggregator. The Client Device periodically pushes data about the usage context and actions and pushes it to the Data Aggregator. The latter will be continuously observing user behavior and generates an authentication score based on the recent and past behaviors of the user. Authentication Consumer registers policies on how to handle each request, with Authentication Engine.

When the Client Device requests for a service from Authentication Consumer, this request is redirected to an Authentication Engine. Prior to the authentication request, authentication consumer would have registered policies with authentication engine, with each policy consisting of an access request, information to be gathered from the client device or data aggregator in relation to this particular request and a rule to decide the result of the request. Upon the request from the Authentication Consumer, Authentication Engine collects relevant information from the Client Device or the Data Aggregator and sends the result to the Authentication Consumer. The service is provided if the authentication score is above a pre-fixed threshold; else, further authentication (typically, a PIN) is required by the user. The authors further describe the implementation of this TrustCube framework with client side engine on Android, Authentication Engine service deployed as Amazon EC2 and encapsulated as AMI, and a web server as Authentication Consumer. The results, in case of device theft, are compared with a simple timed lock-out policy. Based on the rate of false positives (an adversary is successfully authenticated) and false negatives (authentication fails for a legitimate user), the implicit authentication shows considerable improvement over the latter.

Biometrics-based schemes form a major chunk of the user profile methods. Rassan et al. discusses fingerprinting as a possible authentication method in [11]. The paper briefly discusses similar user authentication methods using handwriting [12], a quick response code based on user's image [13] and proceeds to the design and implementation of the proposed method. It has an enrolment phase, where the fingerprint sample is taken using a mobile device camera. This is stored in a database after preprocessing. When a user attempts to login, a fingerprint sample is again taken and is matched with the corresponding entry in the database after preprocessing. The access is granted if the similarity score between the two samples is above a pre-fixed threshold value. The scheme is implemented and processing and enrolment times in various mobile devices (Samsung Galaxy S3, Sony Xperia S and BlackBerry Z) are discussed and compared.

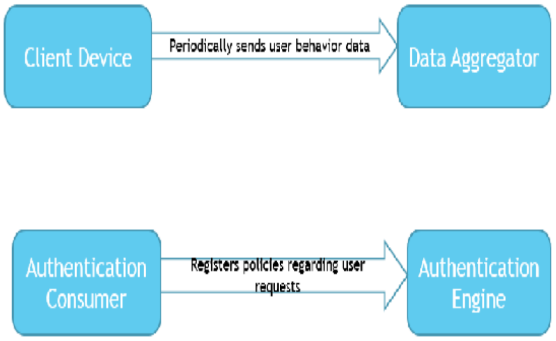
Client Device
Periodically sends user behavior data
Data Aggregator
Authentication Consumer
Registers policies regarding user requests
Authentication Engine

Figure 2. Implicit authentication: Before the request

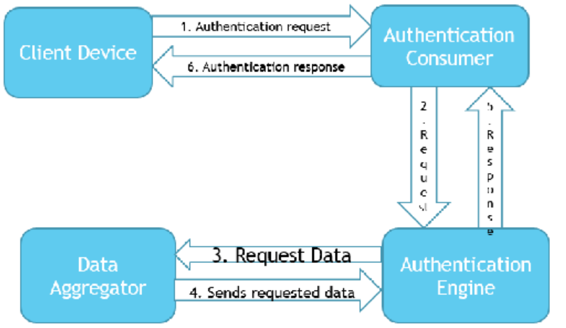

Figure 3. Implicit authentication: Processing the request

In a similar work in [14], Al-Hamami and Al-Juneidi presents an authentication based on passwords and fingerprints. Each fingerprint is associated with a password, which is the combination of a fixed password and a string indicating the sequence of that specific finger. Thus, the user in effect has to remember and securely store only one password. The fingerprint for all ten fingers are stored, together with the associated password. The registration and verification phases are similar to the method described in [11], the difference being the inclusion of the additional password.

Keystroke authentication is a behavioral biometric feature which has been recently discussed as an authentication parameter [15], [16]. Babaeizadeh et al. in [17] presents a method to authenticate users in mobile cloud environment using keystroke pattern. Among the various parameters associated with keystroke biometrics, keystroke duration is chosen as the authentication base in this method. At a successful user registration, the keystroke duration is stored in a database. A tolerance limit for the duration is set. The session's expiration time is set to force the user to login to the system at the end of session. This helps protect the system against session hijacking by an unauthorized person. The scheme is implemented and was successful in preventing unauthorized access in case of keystroke not matching even though the username and password were entered correctly. The results shows the method to be 97.014% correct.

Jeong and Choi proposes the inclusion of user profile data in authentication in [18]. The paper examines a few traditional authentication mechanisms in the context of cloud computing and presents user profiling as a possible alternative. A DTD of the user profile is given, consisting of data concerning the user (name, ID, personal inclination, hobby etc.) and the service (service name, provider name, context, frequency value etc.). However, the proposal in this paper is in rudimentary stage with no details about the framework required.

4.2. Cryptographic methods

Cryptographic methods have been traditionally used for user authentication in various computing platforms. There are several similar methods proposed for mobile cloud computing scenarios too. They typically involve exchange of keys or establishment of tickets with a trusted third party and use the same for establishment of identity.

Local authentication is the method in which the mobile user is authenticated in his/her mobile network. Momeni describes a lightweight local authentication scheme in [19] which consists of two phases: registration and mutual authentication. In the first phase, mobile user provides IMSI and a personal secret information to the mobile service provider and receives an Authentication certificate. Whenever the user wants to use the mobile network services, (s)he encrypts the login request message using the key provided in the first phase and sends it to the provider. A session key is established and is used for further message exchange. A security analysis of this scheme is given, checking the robustness of the system against several attacks.

Shelke and Soni describe an enhanced authentication scheme based on Kerberos in [20]. The high-level architecture consists of three participant modules: An android application, Authentication Server and a Service Server. The Authentication Server issues tickets to users which is used for accessing the service. The paper only presents a very high level scheme for authentication using Kerberos and leaves out the details on establishing the secure channel between application and authentication server and how the Service Server module verifies the authenticity of the ticket.

Meshach and Babu [21] discusses some authentication tools such as signature tokens, Open ID etc. and presents a Mobile Cloud Key Exchange (MCKE) system for mobile cloud systems. It is more focused on security in scheduling of scientific applications across multiple server instances. This scheme needs a Certificate Authority as in Public Key Infrastructure. Participants are issued certificates signed with a public key, so that the certificates and hence the identity of the party can be verified (through the signatures). The cloud controller (CLC), decides which server instances are to be involved in performing the new task and establishes a key between itself and each of these server instances. This scheme is simulated and results are compared with a trivial system based on Internet Key Exchange. MCKE is found to almost halve the runtime on the Cloud Controller compared to IKE.

Kaushik, Awashti, Goel and Goel presents an OTP-based authentication shceme for mobile cloud computing scenarios in [22]. The method basically considers the mobile device as the primary authentication device. The user enters a 4-digit PIN. A java application running on the phone generates an OTP using this PIN, a secret random number (stored only in the phone) and a timestamp; these three components are hashed together with MD5. This OTP and username is sent over the network to the authentication server which grants or denies the requested service access. An advantage is the only secret information passed through the network is the OTP which holds little value for a replay-attacker.

Zhang et al. discussed the idea of elastic devices in [23] which are consumer electronic devices attempting to overcome the resource limits by integration with cloud resources. A typical elastic application has one or more weblets. Reference [23] focusses on the security issues in designing an elastic framework, in particular, the authentication, secure session management authorization, logging of weblet behavior and installation and execution of trusted weblet containers. When a request to launch a weblet is invoked by the user, the Device Elastic Manager generates a pair of weblet session key and weblet session secret. They are shared by all weblets in a session.

The URL of a weblet can be passed to any other weblet that wants to communicate. A calling weblet creates a HMAC (Hash-based Message Authentication Code) with a nonce, its weblet id (wid), target wid and its weblet session secret (wss). The responding weblet first verifies the HMAC with wss and responds based on the verification result. Though the proposed system ensures secure runtime communication between weblets, it assumes that DEM launches weblets only for authenticated application (authentication between user and DEM) and authentication exists between user device, DEM and the Cloud Fabric Interface (CFI). This requires a continuous inspection of the platform’s integrity.

Location Based Services are gaining prominence in the mobile applications scenario. In [24], Zhu et al. discussed the challenges in ensuring security in the location based services in mobile cloud. The authors proposes a framework based on a spatio-temporal predicate based encryption scheme. The scheme is implemented and the computational overheads are analyzed.

It is a desirable feature if a secure communication can be established with a single authentication technique each time the mobile device accesses the cloud from different locations using different networks. In [25], Donald and Arockiam proposes a Unified Cloud Authenticator which is placed between mobile network and Cloud Service Provider, authenticating both. The proposed UCA consists of the following five components: Authentication Server which maintains the credentials of users and CSPs, Hashing Machine, Connection Manager, User Manager and Service Manager. The UCA establishes authentication of user and CSP through digital signatures and public key encryption in three phases: Registration, Authentication and Verification. The username and password are used a credentials in the registration phase. In the authentication phase, the generated key is encrypted and sent to the user. Authentication is done by digital signatures and public key encryption. If the encrypted key is matched during verification, CSP generates an encrypted digital signature to the user for accessing the services.

Dynamic credential system makes use of the randomness and dynamicity in the user-cloud interactions to ensure user identity protection. [26] and [27] discusses generating and updating dynamic credentials in mobile cloud environments.

4.3. Image-based methods

Schwab and Yang proposes a novel authentication scheme for mobile cloud computing entities in [28]. This system integrates certain techniques such as fuzzy vault, picture authentication and zero-knowledge authentication. The paper briefly describes each of these terms to provide background knowledge. In fuzzy vault, a secret k is locked with a key A can be opened by another key B which is “substantially similar” to A. Picture authentication is a visual cryptographic scheme where an image is divided into n transparencies; with any k (where k<n) the hidden image can be retrieved, whereas with k-1 transparencies a user can gain no knowledge about the image or the other transparencies. Finally, in zero knowledge system, an entity can prove he knows a secret without revealing the secret to an observer.

A secure channel for communication between the mobile device and server are set up using Diffie-Hellman key exchange. The user submits a username and 7 image selections, each of which correspond to a number between 1 and 255. This password, with 5 error correcting codes, are considered to be coefficients of a polynomial which is evaluated at several values. At login, 7 image selections, the error correcting codes are added and the polynomial with these numbers as coefficients is evaluated. If the values match with the stored ones, the user is authenticated. A security analysis in the paper shows this system to be resistant against man-in-the-middle, sniffing, replay and data modification attacks. An attacker is shown to have only a probability of $1.95*10^{-11}$ of randomly guessing a correct password.

Quick Response code (QR code) is a two-dimensional barcode which is capable of containing significant amount of information. There have been several attempts to develop QR code-based authentication in mobile devices. Oh, Kim and Lee propose a QR code based authentication method for mobile cloud computing in [13]. In the proposed system, QR code is generated with the username, password and user’s image and is utilized as an authentication certificate.

4.4. Port-knocking methods

In port-knocking authentication method, the client sends no-reply synchronization packets (SYN) to the closed ports of the server firewall. The sequence of ports to which the packets are sent can be selected statically or dynamically. This sequence is logged by the server and is a secret key which, when validated opens the appropriate server (and corresponding service) for the port-knocker client. Reference [29] presents a comprehensive survey of the port-knocking authentication methods which authenticate the user by sending packets to the sequential ports of server. The discussed methods are compared based on the platforms, protocols, and existence of third party dependency.

Virtualization of port-knocking is proposed in [30], which is evaluated using a mathematical model. Central to this improved idea is the concept of Knocked Virtual Machines (KnVM) which, combined with the cloud gateway, keep track of the packets till a sequence is received.

5. Comparative analysis and observations

Table 2 summarizes and compares the surveyed methods for authentication, highlighting the advantages, disadvantages and implementation stage of each. In most of the works, the authors have sketched out the likely direction of future research. In some works, [11, 14, 17, 21, 23, 27] it is the future works suggested is the extension/modification of the existing methods whereas in a few others [18, 20, 26, 30] it is implementation and evaluation of the proposed method in the mobile cloud environment. Only seven of the fourteen discussed methods present an implementation of the proposed framework. Particularly, we note the implicit authentication in [7] as a promising method; it relies on a multitude of user behavior observations to reach the authentication decision, rather than a single factor. It is, to the best of our knowledge, the only proposed method which employs machine learning algorithms to dynamically improve the decision-making process. However, it poses a potential security threat of the stored user information being misused. We suggest the method can be further improved by cryptographically securing the stored usage context and actions. Works such as [31] on privacy-preserving implicit authentication could be considered for adaptation into MCC to achieve this.

Table 2. Comparison of various authentication methods in mobile cloud computing

	Year	**Authentication method**		**Advantage**	**Disadvantage**	**Implemented?**	**Future Work suggested by reference paper authors**
		Type	***Technique***				
Chow et al. [7]	2010	User profile	Implicit authentication by user behavior	Flexible; authentication service resides in cloud	Info collected for authentication is of sensitive nature; need secure storage	Yes	NIL
Rassan et al. [11]	2013	User profile	Finger printing	No extra hardware needed; storage in cloud	Injury may change fingerprinting patterns	Yes	Log file to record unauthorized attempts
Al-Hamami and Al-Juneidi[14]	2015	User profile	Finger printing	No extra hardware needed; extra security with passwords	Injury may change fingerprinting patterns	No	Reading low resolution fingerprints; Completing matching process inside mobile device
Babaeizadeh, Bakhtiari and Maarof[17]	2014	User profile	Keystroke Duration	Cheapest biometric; no extra hardware needed;	Injury, fatigue of user or change in hardware may affect results	Yes	Include other keystroke parameters; investigate false rejection rate
Jeong and Choi[18]	2012	User profile	User and service info	Service info included	Parameters can be easily obtained by attacker	No	Implementation of the proposed method
Momeni [19]	2014	Cryptographic	Local authentication	Lightweight; low latency	No details on establishing secure channel	No	NIL
Shelke and Soni [20]	2015	Cryptographic	Kerberos	Kerberos in mcc context	No details on establishing authentication server	No	Implementation with link to link encryption
Meshach and Babu[21]	2013	Cryptographic	Mobile Cloud Key Exchange	Extends IKE; suitable for scientific application scheduling	Assumption on existence of Certification Authority	Yes	Incorporate cost-efficient encryption
Kaushik, Awashti, Goel and Goel [22]	2012	Cryptographic	Two factor authentication with OTP	Resistant to replay attacks; easy to implement and user friendly	Mobile device and the PIN should be kept securely	Yes	NIL
Zhang et al.[23]	2010	Cryptographic	Secret key exchange	Simple system for security of elastic devices	Details of authentication between user, DEM,CFI omitted	No	Approach to authorize weblets to access sensitive data
Zhu, Ma, Huang and Hu[24]	2013	Cryptographic	Spatio-temporal predicate based encryption	Authentication and security in location based services	LBS servers learning user’s private info can be exploited by attacker	Yes	NIL
Xiao and Gong[26]	2010	Cryptographic	Dynamic credential	User mobility is used to provide authentication	User on the move needs to update dynamic credential frequently	No	Algorithms to be tested in practical mobile cloud environments
Khan, Kiah, Madani, Khan and Ali[27]	2013	Cryptographic	Dynamic Credential	Improved energy usage and processing time compared to [25]	Trusted entity may become processing bottleneck	Yes	A scheme in which trusted entity has reduced processing burden
Schwab and Yang[28]	2012	Picture authentication	Fuzzy picture password	Robust against many known attacks including sniffing, brute force	Might need user familiarization to the password choosing technique	No	NIL
Oh, Kim and Lee[13]	2011	Picture authentication	QR code	Fast processing; capable of error correction	No details on QR code generation steps	Yes	Further research on QR code authentication performance
Boroumand, Shiraz, Gani, Khokhar[30]	2014	Port-knocking	Virtualized port-knocking	Decrease in buffering load to the cloud gateway	Increase in time for authentication	Mathematical modeling and analysis done	Combining dynamic length knocking sequence with virtualization

6. Conclusion

The advent of smartphones and ubiquitous internet connectivity has heralded a paradigm shift in the computing arena. Mobile devices have become a key platform for computation in the recent years, more so with the emergence of mobile cloud computing. With the storage and data processing offloaded to powerful resources in the cloud, mobile devices are fast overcoming their performance constraints. However, to become a stable and effective computing platform, mobile cloud computing must address several issues, security and privacy chief among them. Particularly, the theoretical and practical aspects of an efficient authentication system in mobile cloud computing is a rapidly developing research focal area of recent times.

In this paper, we have presented a comprehensive survey of the major mechanisms proposed so far for authentication in mobile cloud computing. We have proposed a taxonomy for the surveyed authentication mechanisms, which classifies them into four categories: User profile, Cryptographic, Image-based and Port-knocking methods. The basic principles behind the methods are outlined and the pros and cons with the proposed future work are presented in a table for easy reference.

Establishing a robust and efficient authentication mechanism in mobile cloud computing will accelerate its acceptance as a trusted platform for diverse applications. In particular, the implicit authentication which employs machine learning of user behavior holds great future promise. The threat of misuse of stored user behavior data can be addressed by applying cryptographic security constructs. We recommend this approach to be pursued as a research focal area to develop a robust, user-friendly mechanism to effectively address the authentication aspect of secure mobile cloud computing.

7. References

[1] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, and A. Ghalsasi, “Cloud computing – The business perspective,” Decision Support Systems, Volume 51, Issue 1, pp. 529-551, April 2011.

[2] IBM 2013 Annual Report, “The IBM Strategy: We are remaking enterprise IT for the era of cloud,” Available at https://www.ibm.com/annualreport/2013/strategy-cloud.html

[3] International Data Corporation (IDC) Worldwide Quarterly Cloud IT Infrastructure Tracker, “Worldwide Cloud IT Infrastructure Market Growth Expected to Accelerate to 21% in 2015, Driven by Public Cloud Datacenter Expansion, According to IDC,” Press Release, 21 April 2015.

[4] N. Fernando, S. W. Loke, W. Rahayu, “Mobile cloud computing: A survey”, Future Generation Computer Systems, Vol. 29, issue 1, January 2013, Pages 84-106, ISSN 0167-739X.

[5] A.N. Khan, M.L. Mat Kiah, S. U. Khan, and S. A. Madani, “Towards secure mobile cloud computing: A survey,” Future Generation Computer Systems, vol. 29, issue 5, pp. 1278-1299, July 2013.

[6] M. Alizadeh, W. H. Hassan, and T. Khodadadi, "Feasibility of Implementing Multi-factor Authentication Schemes in Mobile Cloud Computing," 2014 Fifth International Conference on intelligent systems, modelling and simulation (ISMS), pp. 615-618, 27-29 Jan. 2014.

[7] R. Chow et al., “Authentication in the clouds: A framework and its application to mobile users,” Proceedings of the 2010 ACM workshop on cloud computing security workshop, pp. 1-6, 2010.

[8] M. Jakobsson, E. Shi, P. Golle, and R. Chow, “Implicit authentication for mobile devices,” HotSec:09: Proceedings of the 4th USENIX workshop on hot topics in security, 2009.

[9] E. Shi, Y. Niu, M. Jakobsson, and R. Chow, “Implicit authentication through learning user behavior,” Information Security Conference (ISC), 2010.

[10] Z. Song, J. Molina, S. Lee, H. Lee, S. Kotani, and R. Masouka, “TrustCube : An infrastructure that builds trust in client,” Future of trust in computing, Proceedings of the first international conference, 2009.

[11] I. Rassan, and H. Shaher, "Securing Mobile Cloud Using Finger Print Authentication", International Journal of Network Security & Its Applications (IJNSA), vol. 5, no. 6, pp.41-53, 2013.

[12] F. Omri, R. Hamila, S. Foufou, and M. Jarraya, “Cloud-ready biometric system for mobile security access,” Networked Digital Technologies, pp. 192-200, 2012.

[13] D. S. Oh, B. H. Kim, and J. K. Lee, “A study on authentication system using QR code for mobile cloud computing environment,” Future Information Technology, pp. 500-507, 2011.

[14] A. H. Al-Hamami, J. Y. Al- Juneidi, “Secure Mobile Cloud Computing Based-On Fingerprint,” World of Computer Science and Information Technology Journal (WCSIT) ISSN: 2221-0741 Vol. 5, No. 2, 23-27, 2015.

[15] P. S. Teh, B. J. T. Andrew, and Y. Shigang, “A survey of keystroke biometrics,” The scientific World Journal, Article ID : 408280, 2013.

[16] M. Choras, and M. Piotr, “Keystroke dynamics for biometric identification,” Adaptive and Natural Computing Algorithms, pp. 424-431. Springer Berlin Heidelberg, 2007.

[17] M. Babaeizadeh, M. Bakhtiari, M. A. Maarof, “Keystroke dynamic authentication in mobile cloud computing,” International Journal of Computer Applications, vol. 90, no. 1, pp. 29-36, March 2014.

[18] H. Jeong, E. Choi, “User authentication using profiling in mobile cloud computing,” Elsevier 2, 262-267, 2012.

[19] M. R. Momeni, “A lightweight authentication scheme for mobile cloud computing,” International Journal of Computer Science and Business Informatics, vol. 14, no. 2, pp. 153-160, 2014.

[20] F. M. Shelke, and P. D. Soni, “An enhanced authentication strategy for multiservice authorization over mobile cloud,” International Journal on Recent and Innovation Trends in Computing and Communication, vol. 3, issue 3, pp. 1669-1672.

[21] W. T. Meshach, and K. S. S. Babu, “Secured and efficient authentication scheme for mobile cloud,” International Journal of Innovations in Engineering and Technology, vol. 2, issue 1, February 2013.

[22] A. Kaushik, H. O. Awashti, K. Goel, and S. Goel, “Secure Authentication with Encryption Technique for Mobile on Cloud Computing,” International Journal of Scientific Research Engineering & Technology (IJSRET) Volume 1 Issue 5 pp 028-033 August 2012

[23] X. Zhang, J. Schiffman, S. Gibbs, A. Kunjithapatham, and S. Jeong., “Securing elastic applications on mobile devices for cloud computing,” Proceedings of the 2010 ACM Cloud Computing Security Workshop, CCSW ’10, November 13, 2009, pp. 127-134.

[24] Y. Zhu, D. Ma, Di. Huang, C. Hu, “Enabling secure location-based services in mobile cloud computing,” Proceedings of the Second ACM SIGCOMM workshop on mobile cloud computing (MCC ‘13), pp. 27-32. 2013.

[25] C. A. Donald, and L. Arockiam, “A unified cloud authenticator for mobile cloud computing environment,” IJCA Proceedings on International Conference on Advanced Computing and Communication Techniques for high performance applications ICACCTHPA, pp. 29-34, February 2015.

[26] S. Xiao, and W. Gong, “Mobility can help : protect user identity with dynamic credential,” 2010 Eleventh International Conference on Mobile Data Management, pp. 378-380, 23-26 May 2010.

[27] A. N. Khan, M. L. Mat Kiah, S. A. Madani, A. R. Khan, M. Ali, “Enhanced dynamic credential generation scheme for protection of user identity in mobile cloud computing,” The Journal of Supercomputing, vol. 66, issue 3, pp. 1687-1706, December 2013.

[28] D. Schwab, L. Yang, “Entity authentication in a mobile-cloud environment,” CSIIRW ’12, Oct 30 – Nov 01, 2012, Oak Ridge, TN, USA ACM 978-1-4503-1687-3/12/10.

[29] L. Boroumand, M. Shiraz, A. Gani, S. Khan, S. A. A. Shah, “A review on port-knocking methods for mobile cloud computing,” The Scientific World Journal, in press.

[30] L. Boroumand, M. Shiraz, A. Gani, S. Khan, R. Khokhar, “Virtualization Technique for port-knocking in mobile cloud computing,” Int. J. Advanced Soft Comput. Appl., vol. 6, no. 1, 2014.

[31] N. A. Safa, R. Safavi-Naini, S. F. Shahandashti, “Privacy preserving implicit authentication,” Proceedings of 29th IFIP TC 11 International Conference, SEC 2014, Marrakech, Morocco, June 2-4, 2014. pp. 471-484.